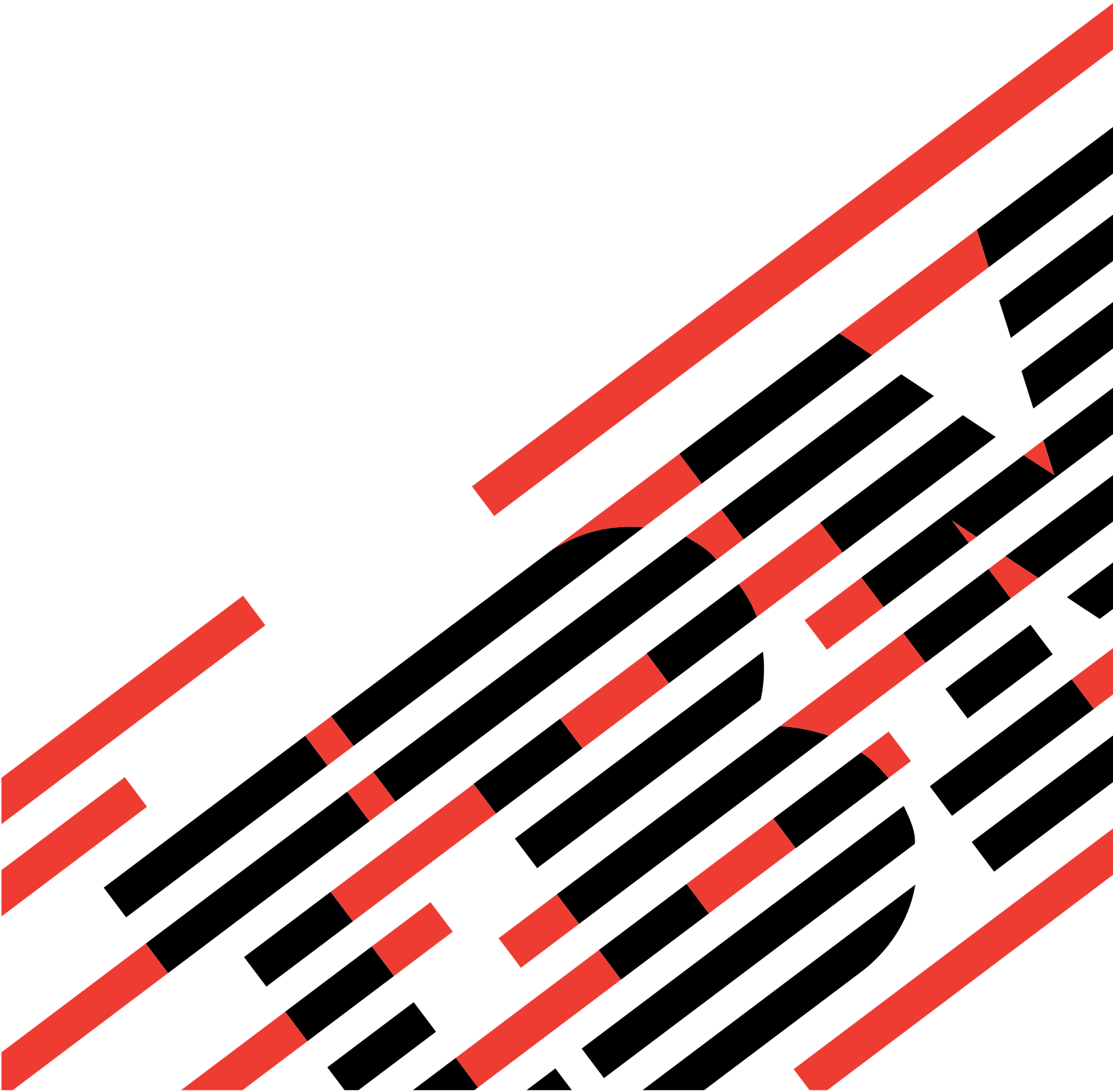
IBM

eserver

iSeries

# Устранение неполадок TCP/IP

*Версия 5*



IBM

@server

iSeries

# Устранение неполадок TCP/IP

*Версия 5*

# Содержание

# Глава 1. Устранение неполадок TCP/IP

Что препятствует работе TCP/IP? Вы спланировали конфигурацию сети и выполнили все инструкции, однако по каким-то причинам начать работу с TCP/IP не удается. Ответы вы найдете в этом разделе.

Данный сайт является отправной точкой при выяснении причин неполадок TCP/IP. Если неполадка связана с соединением, то ее легко обнаружить; если же неполадка носит локальный характер, то может потребоваться более углубленный анализ. Ниже рассмотрены различные средства и приемы, позволяющие найти и устранить неполадку.

**Новое в версии V5R2**
Этот раздел содержит информацию об изменениях и дополнениях в способах устранения неполадок TCP/IP.

**Как напечатать это раздел**
В этом разделе приведены инструкции по печати и загрузке PDF-версии документации Устранение неполадок TCP/IP.

**Общие неполадки TCP/IP**
Этот раздел посвящен проверке соединений TCP/IP. Система ″вопрос-ответ″ поможет вам идентифицировать неполадку и выбрать способ ее устранения.

**Неполадки, связанные с конкретными приложениями**
Если известно, что неполадка связана с конкретным приложением, например с FTP или DNS, то этот раздел поможет вам выбрать способ устранения такой неполадки.

**Трассировка линии связи**
Этот раздел содержит инструкции по сбору данных трассировки линии связи. Трассировка позволяет локализовать неполадку, что упрощает ее устранение. Вы можете сами воспользоваться информацией трассировки или передать ее специалистам фирмы IBM.

**Файлы конфигурации TCP/IP**
Этот раздел содержит информацию о том, каким образом можно скопировать файлы конфигурации TCP/IP. Эти копии необходимо будет предоставить специалистам фирмы IBM, если вы решите обратиться к ним за помощью.

**Протокол работы продукта**
В этом разделе приведена информация о том, каким образом протокол работы продукта может помочь вам при анализе неполадки.

## Новое в версии V5R2

В версии V5R2 в раздел Устранение неполадок TCP/IP добавлены следующие пункты:

- **Общие неполадки TCP/IP**
  Информация об устранении неполадок, связанных с Протоколом Internet IPv6.
- **Трассировка линии связи**
  Информация о трассировке линии связи с помощью команд CL. Это средство устранения неполадок выполняет трассировку данных, передаваемых по линии связи, что позволяет определить причину неполадки.

Дополнительная информация о изменениях и дополнениях в этом выпуске приведена в документе Информация для пользователей  .

## Как напечатать этот раздел

Для просмотра или загрузки версии в формате PDF выберите Устранение неполадок TCP/IP (около 152 Кб, или 26 страниц).

Для сохранения файла в формате PDF на рабочей станции с целью последующего просмотра или печати выполните следующие действия:

1. Щелкните правой кнопкой на файле PDF в браузере (щелкните на приведенной выше ссылке).
2. Выберите **Сохранить как...**.
3. Укажите каталог, в котором вы хотите сохранить документ.
4. Нажмите кнопку **Сохранить**.

### Загрузка программы Adobe Acrobat Reader

Копию программы Adobe Acrobat Reader, необходимую для просмотра и печати документов в формате PDF, можно загрузить с Web-сайта фирмы Adobe (www.adobe.com/prodindex/acrobat/readstep.html) .

# Глава 2. Общие неполадки TCP/IP

Этот раздел содержит описание нескольких способов устранения неполадок. Эти способы позволяют локализовать неполадки и проверить соединения TCP/IP. Если соединения TCP/IP уже проверены и точно известно, что неполадка связана с определенным приложением, перейдите к разделу Неполадки, связанные с конкретными приложениями.

**Предварительный анализ неполадок TCP/IP**
Эта информация содержит ряд инструкций и вопросов, которые помогут определить причину возникновения неполадки.

**Сведения о команде PING**
Это подробное описание команды PING и способов ее применения.

**Работа с протоколом задания и очередями сообщений**
Этот раздел содержит сведения еще об одном способе устранения неполадок TCP/IP.

## Предварительный анализ неполадок TCP/IP

Эти вопросы и ответы позволяют провести анализ неполадки, определить ее причину и возможные способы устранения. Для продолжения процесса устранения неполадки перейдите по ссылке к одному из списков причин.

1. Вызовите команду PING для хоста в локальной сети. Команда была выполнена успешно?
   a. Да. Перейдите к шагу 2.
   b. Нет. Перейдите к Списку причин A.
2. Вызовите команду PING для удаленной системы. Команда была выполнена успешно?
   a. Да. Перейдите к шагу 3.
   b. Нет. Перейдите к Списку причин B.
3. Проверьте, запущены ли в подсистеме QSYSWRK все необходимые задания TCP/IP. Все ли задания запущены?
   a. Да. Перейдите к шагу 4.
   b. Нет. Перейдите к Списку причин C.
4. Проверьте с помощью NETSTAT, работает ли интерфейс. Интерфейс работает?
   a. Да. Перейдите к шагу 5.
   b. Нет. Перейдите к Списку причин D.
5. Убедитесь с помощью TELNET или FTP, что маршруты TCP/IP правильно настроены. Кроме того, проверьте с помощью NETSTAT, установлено ли соединение. Соединение установлено?
   a. Да. Запустите приложение.
   b. Нет. Перейдите к Списку причин E.

## Список причин A

Учтите, что в удаленной системе может быть отключен режим ответов ICMP. В этом случае вы не получите ответ от удаленной системы, даже если соединение исправно. Если вы считаете, что неполадка вызвана сбоем соединения, попытайтесь проверить соединения с другими удаленными системами, а также соединения между различными удаленными системами, чтобы как можно точнее локализовать неполадку.

1. Убедитесь, что протокол TCP/IP активен в локальной системе.
   Выполните следующие действия для запуска стека TCP/IP:

a. Введите команду STRTCP. Если протокол активен, вы получите сообщение TCP1A04 (Протокол TCP/IP в данный момент активен). В противном случае команда STRTCP запустит протокол TCP/IP на локальном сервере. Убедитесь, что запуск TCP/IP прошел без ошибок.

b. В разделе Способы устранения неполадок IPv6 приведена информация о способах устранения неполадок IPv6. Если применяется другая версия протокола, перейдите к следующему пункту.

2. Проверьте правильность работы программного обеспечения TCP/IP.

   Для проверки работы программного обеспечения TCP/IP на сервере зарезервированы имя хоста LOOPBACK и интерфейс, связанный с описанием линии *LOOPBACK. Если вы укажете имя хоста LOOPBACK, то реально данные не будут передаваться ни по одной из подключенных физических линий связи. Таким образом вы можете быстро определить, правильно ли работает протокол TCP/IP.

   Для проверки правильности работы протокола TCP/IP выполните следующие действия:

   a. Убедитесь, что локальная таблица хостов содержит запись с именем хоста LOOPBACK и IP-адресом 127.0.0.1.

   b. Убедитесь, что интерфейс, сопоставленный с хостом LOOPBACK, активен. Обычно интерфейсу LOOPBACK соответствует IP-адрес 127.0.0.1. Убедитесь, что в конфигурации интерфейса с IP-адресом хоста LOOPBACK задано описание линии *LOOPBACK. Введите команду:

      ```
      NETSTAT OPTION(*IFC)
      ```

      для определения состояния интерфейса LOOPBACK. Если он неактивен, выберите опцию 9 для его запуска.

   c. Убедившись, что интерфейс хоста LOOPBACK активен, введите следующую команду:

      ```
      PING RMTSYS(LOOPBACK)
      ```

      Хост LOOPBACK дает пользователю возможность:

      - Проверять правильность работы FTP, TELNET, LPR и пользовательских программ без подключения к физической линии связи или сети.
      - Проверять правильность установки и функционирования программного обеспечения TCP/IP.

      Для проверки соединения с другим локальным IP-адресом воспользуйтесь командой PING.

   d. Для тестирования программного и аппаратного обеспечения (правильности подключения адаптера и сети) укажите IP-адрес внешнего хоста в сети:

      ```
      PING RMTSYS('nnn.nnn.nnn.nnn')
      ```

   e. Если проверить правильность подключения локальной системы к сети, задавая имя или IP-адрес этой системы, не удается, просмотрите список записей исходной служебной точки доступа (SSAP) в описании линии связи, связанном с сетевым интерфейсом. Данный список должен содержать запись X'AA'. При создании нового описания линии связи эта запись добавляется по умолчанию, при условии что параметру SSAP присвоено значение по умолчанию *SYSGEN. Если вы работаете с уже существующим описанием линии, вы можете добавить нужную запись в список с помощью команды Изменить описание линии связи.

      Поскольку записи об исходных служебных точках доступа (SSAP) для TCP/IP предусмотрены не для всех типов линий связи, проверьте список записей SSAP в описании линии связи, связанном с интерфейсом.

   f. Проверьте правильность всех параметров описания линии связи. Обратите особое внимание на размер кадра (он должен быть не меньше максимального размера блока передачи (MTU) для данного интерфейса).

   g. Если вам не удается получить ответное сообщение от удаленной системы, это может означать, что данная система, сеть, внешний хост или мост недоступны или работают неправильно. Возможно также, что в удаленной системе отключен режим ответов ICMP. Это может произойти в случае, если удаленная система выполняет роль брандмауэра и, согласно настройке, не отвечает на запросы ICMP. Попытайтесь проверить соединения с другими

удаленными системами, а также соединения между различными удаленными системами, чтобы как можно точнее локализовать неполадку.

h. Убедитесь, что локальный интерфейс настроен правильно.

i. Если интерфейсы TCP/IP (в том числе, интерфейс LOOPBACK) не удается активизировать, или если вы не можете завершить или запустить протокол TCP/IP, убедитесь, что в описании подсистемы QSYSWRK заданы две указанные ниже записи маршрутизации. Если эти записи отсутствуют или неверны, добавьте или исправьте их, а затем повторите операцию.

```
ADDRTGE  SBSD(QSYS/QSYSWRK) +
         SEQNBR(2505) +
         CMPVAL(TCPIP) +
         PGM(QSYS/QTOCTCPIP) +
         CLS(QSYS/QSYSCLS20) +
         MAXACT(*NOMAX) +
         POOLID(1)

ADDRTGE  SBSD(QSYS/QSYSWRK) +
         SEQNBR(2506) +
         CMPVAL(TCPEND) +
         PGM(QSYS/QTOCETCT) +
         CLS(QSYS/QSYSCLS20) +
         MAXACT(*NOMAX) +
         POOLID(1)
```

Вернитесь к разделу Предварительный анализ неполадок TCP/IP и продолжите устранение неполадки.

## Способы устранения неполадок IPv6

Эти способы предназначены для устранения неполадок сети IPv6.

1. Убедитесь, что протокол TCP/IP запущен.
   a. Убедитесь в том, что циклический интерфейс настроен и работает. Для проверки состояния циклического интерфейса выполните следующие действия:
      1) В Навигаторе iSeries разверните **значок сервера—> Сеть —> Конфигурация TCP/IP —> IPv6 —> Интерфейсы**.
      2) Найдите циклический интерфейс в правой панели. Циклическому интерфейсу IPv6 соответствуют IP-адрес ::1 и имя линии Loopback 6. Если циклического интерфейса нет в списке, то необходимо настроить его с помощью мастера **Настройки IPv6**.
   b. Отправьте пробный пакет по циклическому адресу (::1). Сервер отправляет самому себе пакет IPv6 и таким образом проверяет работу стека IPv6. Для проверки стека с помощью утилиты Ping выполните следующие действия:
      1) В Навигаторе iSeries разверните **значок сервера —> Сеть**.
      2) Щелкните правой кнопкой мыши на пункте **Конфигурация TCP/IP**, выберите **Утилиты**, а затем **Ping**.
2. Проверив работу стека IPv6, убедитесь в том, что линия IPv6 настроена и работает. Это может быть линия Ethernet или настроенная туннельная линия.

   Для проверки состояния линий, настроенных на сервере, выполните следующие действия:
   a. В Навигаторе iSeries разверните значок **сервера —> Сеть —> Конфигурация TCP/IP —> Линии**.
   b. В правой панели найдите линию, которая должна быть настроена для IPv6, и проверьте значение в столбце Состояние. Если этой линии нет в списке, то ее необходимо настроить с помощью мастера **Настройки IPv6**. Инструкции по настройке линии для IPv6 приведены в разделе Настройка IPv6. Если линия указана в списке и значение ее состояния - **Не загружена**, то это означает, что линия настроена, но не загружена в конфигурацию стека IPv6. Для определения причин неполадки введите команду Работа с описанием линии (WRKLIND) в командной строке.

3. Убедитесь в том, что работают по крайней мере два интерфейса IPv6: локальный интерфейс и тот, которому отправляется пробный пакет.

   Для проверки состояния интерфейсов IPv6 выполните следующие действия:

   a. В Навигаторе iSeries разверните **значок сервера—> Сеть —> Конфигурация TCP/IP —> IPv6 —> Интерфейсы**.

   b. В правой панели найдите IP-адрес, связанный с локальным интерфейсом, и проверьте состояние этого интерфейса.

   c. Если интерфейс **Неактивен**, его необходимо активизировать. Для активации интерфейса щелкните правой кнопкой мыши на IP-адресе и выберите **Запустить**.

   d. Повторите эту операцию для проверки состояния удаленного интерфейса.

4. Если отправить пробный пакет по адресу IPv6 не удалось, проверьте состояние адресов обоих интерфейсов. Адреса обоих интерфейсов должны быть **Предпочитаемыми**. Если один из интерфейсов не является предпочитаемым, то измените состояние этих интерфейсов или выберите для проверки другие интерфейсы.

   Для проверки или изменения состояния адресов исходного интерфейса выполните следующие действия:

   a. В Навигаторе iSeries разверните **значок сервера—> Сеть —> Конфигурация TCP/IP —> IPv6 —> Интерфейсы**.

   b. В правой панели щелкните правой кнопкой на IP-адресе, связанном с этим интерфейсом, выберите **Свойства**, а затем выберите страницу **Опции**. Это окно диалога позволяет указать срок действия предпочитаемого или действительного состояния интерфейса.

   c. Повторите эту операцию для проверки состояния адреса целевого интерфейса.

## Список причин B

Если команда VFYTCPCNN (PING) успешно выполняется в локальной системе, вам следует проверить возможность установления соединения между локальной и удаленной системами. Вызовите команду PING так же, как это было описано выше, но укажите IP-адрес удаленного хоста. Обратитесь к разделу Сообщения об ошибках. Учтите, что в удаленной системе или в брандмауэре может быть отключен режим ответов ICMP. В этом случае вы не получите ответ от удаленной системы, даже если соединение исправно. Если вы считаете, что неполадка вызвана сбоем соединения, попытайтесь проверить соединения с другими удаленными системами, а также соединения между различными удаленными системами, чтобы как можно точнее локализовать неполадку.

1. Если проверка соединения завершается успешно при использовании удаленного IP-адреса, но при указании имени удаленной системы возникает сбой, это может означать, что IP-адрес или имя этой системы неправильно заданы в таблице хостов, или что удаленные серверы имен недоступны.
2. Если локальная система должна обращаться к удаленным серверам имен, убедитесь, что все эти серверы доступны. Для этого воспользуйтесь командой PING, поочередно задавая IP-адреса удаленных серверов имен.
3. В команде PING предусмотрены дополнительные параметры, которые позволяют вам задавать длину пакетов данных, количество отправляемых пакетов, а также время ожидания ответа. По умолчанию время ответа составляет 1 секунду - в большинстве сетей этого промежутка времени удаленной системе вполне достаточно для отправки ответа. Однако, если маршрут к удаленной системе слишком велик, или если сеть сильно загружена, вам может потребоваться задать больший промежуток времени ожидания ответа удаленной системы.

   Рекомендуется не изменять значения, присвоенные параметрам этой команды по умолчанию. Учтите, что если вы укажете большой размер пакета и небольшое время ожидания, сеть, возможно, будет не успевать передавать пакеты в удаленную систему и возвращать ответные пакеты. В этом случае команда PING сообщит о тайм-ауте. Если время ожидания будет

недостаточным для передачи и приема пакетов команды PING, у вас может сложиться ложное впечатление, что установить соединение с удаленной системой невозможно.

4. Если вам не удается получить ответное сообщение от удаленной системы, это может означать, что данная система, сеть, шлюз, маршрутизатор или мост недоступны или работают неправильно. Возможно также, что в удаленной системе отключен режим ответов ICMP. Попытайтесь проверить соединения с другими удаленными системами, а также соединения между различными удаленными системами, чтобы как можно точнее локализовать неполадку.
5. Если с помощью команды PING вам не удается получить ответ от удаленной системы при проверке интерфейса, сопоставленного с описанием линии связи Ethernet, убедитесь, что в описании линии связи Ethernet указан правильный стандарт Ethernet или значение *ALL.
6. Если вы не можете получить ответ ни от одной системы сети, неполадка, вероятно, возникла на одном из участков маршрута. Проверьте соединение со шлюзом, через который локальная система подключена к сети. В случае неудачи последовательно проверяйте доступность удаленных систем, составляющих маршрут, пока не обнаружите точку сбоя.
7. Для передачи пакетов используется низкоуровневый протокол, не гарантирующий доставку. Потеря одного эхо-запроса не означает, что сеть или шлюз недоступны. Это можно предположить с достаточной вероятностью только в том случае, если будут неудачно выполнены несколько команд PING подряд.

Если выполнить команду PING для хоста в удаленной сети не удается, вызовите для той же сети команду Трассировать маршрут (TRACEROUTE). Она позволяет выполнить те же тесты, что и набор отдельных команд Ping, но за один прием. Команда TRACEROUTE проверит все узлы маршрута к удаленной системе и определит, связана ли неполадка с маршрутизатором или с удаленной сетью.

Введите `TRACEROUTE RMTSYS('x.x.x.x')`. Можно указать как IP-адрес, так и имя удаленной системы; например (`'xxxx.xxxx.com'`). Утилита Trace Route поддерживает как формат адресов IPv4 (`'x.x.x.x'`), так и формат IPv6 (`'x:x:x:x:x:x:x:x'`).

Утилиту Trace Route можно также вызвать из Навигатора iSeries. Для запуска утилиты Trace Route выполните следующие действия:

1. В Навигаторе iSeries разверните значок сервера —> **Сеть**.
2. Щелкните правой кнопкой мыши на **Конфигурация TCP/IP**, выберите **Утилиты**, а затем **Трассировка маршрута**.

Вернитесь к разделу Предварительный анализ неполадок TCP/IP и продолжите устранение неполадки.

## Список причин C

1. Убедитесь, что в подсистеме QSYSWRK запущены все необходимые задания (локальные и удаленные). В этой подсистеме должно быть активно по крайней мере задание QTCPIP. Задание QTCPIP управляет запуском и завершением работы интерфейсов TCP/IP. Кроме того, для каждого приложения, которое вы планируете применять, должно быть запущено хотя бы одно задание (пример списка активных заданий приведен на рис. 1 на стр. 8). Возможно, имена этих заданий будут отличаться от имен заданий FTP, LPD и TELNET, выполняющихся в указанной подсистеме. Имена заданий FTP начинаются с `QTFTP`. Имена заданий LPD начинаются с `QTLPD`. Имена заданий TELNET начинаются с `QTVTELNET` и `QTVDEVICE`. В одной подсистеме может быть запущено несколько заданий сервера FTP, LPD или TELNET. Имена заданий SMTP начинаются с `QTSMTP`. Протокол SMTP активизирует до четырех заданий в подсистеме QSYSWRK и два задания в подсистеме QSNADS. Имена заданий SNMP начинаются с `QTMSNMP`. Протокол SNMP активизирует в подсистеме QSYSWRK три задания: QTMSNMP, QTMSNMPRCV и QSNMPSA.

   Вы можете просмотреть список активных заданий, вызвав команду Работа с активными заданиями (WRKACTJOB). Введите `WRKACTJOB SBS(QSYSWRK)`.

2. Если запущены не все требуемые задания, завершите работу протокола TCP/IP, вызвав команду ENDTCP OPTION(*IMMED). Найдите все протоколы, связанные с отсутствующими заданиями.
3. В описаниях всех заданий замените уровень занесения сообщений в протокол на 4 0 *SECLVL. Подробные сведения об уровнях занесения сообщений в протокол приведены в разделе Работа с протоколом задания и очередями сообщений.
4. Повторно запустите TCP/IP с помощью команды STRTCP.
5. Убедитесь, что все необходимые задания активны.
6. Если будут запущены не все задания, просмотрите связанные с ними протоколы.

```
                  Работа с активными заданиями              SYSNAM03

                                    02/03/99  18:06:32
% CPU:     .8   Прошедшее время: 02:21:32     Число активных заданий:   93

Введите опции, нажмите Enter.
  2=Изменить 3=Блокир. 4=Завершить 5=Работа с 6=Разблокир. 7=Показать сообщение
  8=Работа с буферными файлами    13=Отсоединить...

Опц  Подсист./Зад.  Польз.      Тип   % CPU  Функция         Состояние
     QSYSWRK        QSYS        SBS      .0                  DEQW
       QMSF         QMSF        BCH      .0                  DEQW
       QNEOSOEM     QUSER       ASJ      .0  PGM-QNEOSOEM    TIMW
       QNEOSOEM     QUSER       BCH      .0  PGM-QNEOSOEM    TIMW
       QNEOSOEM     QUSER       BCH      .0  PGM-QNEOSOEM    TIMW
       QNPSERVD     QUSER       BCH      .0                  SELW
       QPASVRP      QSYS        BCH      .0  PGM-QPASVRP     DEQW
       QPASVRS      QSYS        BCH      .0  PGM-QPASVRS     TIMW
       QPASVRS      QSYS        BCH      .0  PGM-QPASVRS     TIMW
                                                                Еще...
Параметры или команда
===>
F3=Выход    F5=Обновить       F7=Поиск      F10=Обновить статистику
F11=Показать рабочие данные   F12=Отмена    F23=Доп. опции   F24=Доп. клавиши
```

*Рисунок 1. Меню Работа с активными заданиями — страница 1*

```
                  Работа с активными заданиями              SYSNAM03
                                    02/03/99  18:06:32
% CPU:     .8   Прошедшее время: 02:21:32     Число активных заданий:   93

Введите опции, нажмите Enter.
  2=Изменить 3=Блокир. 4=Завершить 5=Работа с 6=Разблокир. 7=Показать сообщение
  8=Работа с буферными файлами    13=Отсоединить...

Опц  Подсист./Зад.  Польз.      Тип   % CPU  Функция         Состояние
       QTLPD03516   QTCP        BCH      .0                  DEQW
       QTLPD03580   QTCP        BCH      .0                  TIMW
       QTMSNMP      QTCP        BCH      .0  PGM-QTOSMAIN    DEQW
       QTMSNMPRCV   QTCP        BCH      .0  PGM-QTOSRCVR    TIMW
       QTVDEVICE    QTCP        BCH      .0  PGM-QTVDEVMG    TIMW
       QTVTELNET    QTCP        BCH      .0                  TIMW
       QZBSEVTM     QUSER       ASJ      .0  PGM-QZBSEVTM    EVTW
       QZHQSRVD     QUSER       BCH      .0                  SELW
       QZRCSRVSD    QUSER       BCH      .0                  SELW
                                                                Еще...
Параметры или команда
===>
F3=Выход    F5=Обновить       F7=Поиск      F10=Обновить статистику
F11=Показать рабочие данные   F12=Отмена    F23=Доп. опции   F24=Доп. клавиши
```

*Рисунок 2. Работа с активными заданиями — страница 2*

Вернитесь к разделу Предварительный анализ неполадок TCP/IP и продолжите устранение неполадки.

## Список причин D

Функция работы с состоянием сети (NETSTAT) сервера позволяет определять состояние интерфейсов TCP/IP, получать информацию о конфигурации маршрутов TCP/IP, а также определять состояние соединения TCP/IP в локальной системе. Вы можете пользоваться как командой WRKTCPSTS, так и командой NETSTAT.

1. Прежде чем определять состояние сети, запустите протокол TCP/IP с помощью команды `STRTCP`. Если вы не сделаете этого, меню Работа с состоянием сети TCP/IP будет выведено на экран, однако его опции станут доступными только после запуска TCP/IP.
2. Если вы попытаетесь запустить уже активный интерфейс или завершить неактивный в меню Работа с состоянием интерфейса TCP/IP, вы получите сообщение об ошибке. Если интерфейс не удается сделать активным путем выбора опции запуска, возможно, это вызвано сбоем интерфейса, неполадкой на линии связи или ошибкой в конфигурации линии связи. Для получения информации об ошибках, которые, возможно, возникли при активизации интерфейса, просмотрите протокол задания QTCPIP. Кроме того, вы сможете более точно определить состояние сети, просмотрев сообщения в очереди сообщений QSYSOPR и протоколе хронологии QHT (DSPLOG).
3. Введите `WRKCFGSTS *LIN`, чтобы выяснить, вызвана ли неполадка ошибкой в описании линии связи.
4. Убедитесь, что в меню Работа с состоянием соединений TCP/IP каждому из указанных ниже серверов соответствует, по крайней мере, одно пассивное соединение в состоянии прослушивания (для вызова этого меню введите опцию 3 в меню Работа с состоянием сети TCP/IP). Проверьте состояние соединений с серверами, поддерживающими эти приложения, и другими связанными серверами в сети:

   SNMP

   TELNET

   В AS/400 версии 4, выпуск 4, помимо Telnet поддерживается SSL Telnet. По умолчанию SSL Telnet работает с портом 992, а стандартный Telnet - с портом 23. Для отключения стандартного Telnet и обеспечения доступа к SSL Telnet рекомендуется задать ограничения на номера приемных портов Telnet.

   FTP

   SMTP (если настроен)

   POP

   LPD

   REXEC

   HTTP (если настроен)

   Поля *Удаленный адрес* и *Удаленный порт* в записи о пассивном соединении в состоянии прослушивания содержат символ ″звездочка″. Завершать эти соединения не рекомендуется. Удаленные системы не смогут пользоваться SNMP, FTP и TELNET, отправлять в локальную систему почту SMTP и передавать в нее буферные файлы с помощью LPR, если связанные с этими системами пассивные соединения в состоянии прослушивания будут завершены. Для повторного запуска пассивных соединений, связанных с некоторым сервером, необходимо вызвать для этого сервера команду `ENDTCPSVR`, а затем команду `STRTCPSVR`.
5. Убедитесь, что на порты, связанные с приложением, с которым вы планируете работать, не наложено никаких ограничений. Для просмотра списка запрещенных портов введите опцию 4 (Работа с запретами на порты TCP/IP) в меню Настроить TCP/IP.

Вернитесь к разделу Предварительный анализ неполадок TCP/IP и продолжите устранение неполадки.

## Список причин E

Проверьте правильность данных конфигурации. Если конфигурация задана верно, перейдите к разделу Неполадки, связанные с конкретными приложениями и продолжите устранение неполадки для приложения, с которым вы работаете.

## Сведения о команде PING

Подробные сведения о команде PING приведены в следующих разделах.

**Добавление имен доменов к именам хостов**
В этом разделе приведена информация о том, каким образом сервер добавляет к имени хоста имя домена.

**Сообщения об ошибках**
Данный раздел содержит примеры наиболее распространенных ошибок.

## Добавление имен доменов к именам хостов

Приведенный ниже пример показывает, каким образом сервер применяет имя локального домена в качестве списка поиска и добавляет имя домена к имени хоста, если имя домена не оканчивается точкой.

Предположим, что имя локального сервера - SYSNAM01.A400SSC.DFW.COMPANY.COM и нужно проверить соединение с системой SYSNAM02.DFW.COMPANY.COM. Имя хоста SYSNAM02 не задано в локальной таблице хостов.

Если ввести команду `PING SYSNAM02.DFW.COMPANY.COM`, то сервер отправит имя SYSNAM02.DFW.COMPANY.COM удаленному серверу имен.

Если ввести команду `PING SYSNAM02`, то сервер сначала отправит имя SYSNAM02.A400SSC.DFW.COMPANY.COM удаленному серверу имен. Затем будет отправлено имя SYSNAM02.DFW.COMPANY.COM. Если и это имя не будет найдено, сервер отправит имя SYSNAM02.COMPANY.COM. Другими словами, протокол TCP/IP iSeries добавляет к имени хоста каждую часть имени локального домена.

Если ввести команду `PING SYSNAM02.`, то удаленный сервер имен сообщит, что данный хост неизвестен. Удаленный сервер имен не найдет имя SYSNAM02, так как в этом случае сервер отправляет имя SYSNAM02, не добавляя к нему элементы списка поиска. Единственное отличие от предыдущего примера заключается в том, что в конец имени хоста добавлена точка.

## Сообщения об ошибках

Возможно, что при вызове команды PING для проверки соединения с другим хостом сети, протокол TCP/IP вернет сообщение об ошибке. Приведенная ниже таблица содержит описания сообщений об ошибках и инструкции по устранению неполадок.

| Сообщение об ошибке | Необходимые действия |
|---|---|
| Службы TCP/IP недоступны | • Протокол TCP/IP еще не был запущен, либо его запуск еще не завершен. С помощью команды NETSTAT определите, запущен ли протокол TCP/IP.<br>• Возможно, в подсистеме QSYSWRK активизированы еще не все необходимые задания.Введите команду Работа с активными заданиями (WRKACTJOB), чтобы убедиться, что подсистема QSYSWRK и все требуемые задания активны. Если это не так, просмотрите сообщения, находящиеся в протоколе задания или системной очереди вывода по умолчанию. |
| Невозможно установить соединение с удаленным хостом | Проверьте правильность конфигурации интерфейсов, описаний сопоставленных с ними линий связи и маршрутов TCP/IP. |
| Невозможно установить соединение с удаленной системой | Протоколу TCP/IP не удалось найти маршрут к указанному узлу. Проверьте опцию 2 NETSTAT и убедитесь, что сетевой маршрут *DFTROUTE или его эквивалент настроен и работает. |
| Ответ от удаленного хоста не был получен командой VFYTCPCNN в течение 10 секунд, проверка соединения 1. | • Вероятно, конфигурация задана правильно, однако получить ответ от удаленной системы не удается. Убедитесь, что удаленный хост доступен. Свяжитесь с администратором удаленной системы и попросите его проверить соединение с вашей системой.<br>• Проверьте правильность записей таблиц хостов и удаленного сервера имен (если он применяется) в обоих системах, а также правильность интерфейсов и маршрутов TCP/IP. Возможно, удаленный сервер имен не может обработать ваш запрос по какой-либо причине.<br>• При работе с линией связи Ethernet убедитесь, что вы правильно задали стандарт Ethernet или указали значение *ALL. |
| VFYTCPCNN: Хост xxxxxx неизвестен, где xxxxxx - это имя хоста. | Имя хоста не удалось преобразовать в IP-адрес ни с помощью таблицы хостов, ни с помощью сервера имен. Проверьте правильность записи о данном удаленном хосте в локальной таблице хостов или в таблице удаленного сервера имен (если он применяется). |

## Работа с протоколом задания и очередями сообщений

При установке протокола TCP/IP создается несколько описаний заданий.

Описания заданий хранятся в библиотеке QSYS или QTCP. Первоначально для них заданы следующие значения: уровень занесения сообщений в протокол - 4, серьезность сообщений, заносимых в протокол, - 0, текст для операции занесении сообщений в протокол - *NOLIST. Указанное сочетание значений запрещает создание протокола задания, содержащего только сообщения о запуске и завершении этого задания.

Одно из первых действий, которые вам следует выполнить в случае возникновения неполадок в работе протокола TCP/IP, - это изменить уровень занесения сообщений в протокол в описаниях заданий, связанных с приложениями, которые вы хотите применять, и указать в качестве текста для операции занесения сообщений в протокол значение *SECLVL. При изменении уровня занесения сообщений в протокол будет создан протокол задания, соответствующего применяемому

приложению. Для того чтобы изменения вступили в силу, необходимо перезапустить сервер. Однако если вы переопределите уровень ведения протокола активного задания с помощью команды CHGJOB, то изменения сразу вступят в силу.

Изменение уровня занесения сообщений в протокол в описании задания для конкретного приложения продемонстрировано в следующих примерах:

- Если неполадка связана с протоколом FTP, то измените описание задания QTMFTPS с помощью следующей команды CL:

  ```
  CHGJOBD  JOBD(QTCP/QTMFTPS)  LOG(4 0 *SECLVL)
  ```

- Если неполадка связана с протоколом SMTP, то измените описание задания QTMSMTPS с помощью следующей команды CL:

  ```
  CHGJOBD  JOBD(QTCP/QTMSMTPS)  LOG(4 0 *SECLVL)
  ```

  Возможно, вам потребуется изменить уровень занесения сообщений в протокол не только в описании задания QTMSMTPS, но и в описании задания подсистемы QSNADS. Для этого необходимо ввести следующую команду:

  ```
  CHGJOBD  JOBD(QGPL/QSNADS)  LOG(4 0 *SECLVL)
  ```

# Глава 3. Неполадки, связанные с конкретными приложениями

Если вы определили, что неполадка связана с конкретным приложением, работающим с TCP/IP, выберите один из приведенных ниже разделов, содержащих подробные сведения об устранении неполадок. Ссылки в этих разделах позволяют перейти на другие сайты, содержащие информацию по устранению неполадок в соответствующих приложениях.

**Сервер имен доменов (DNS)**
Этот раздел содержит схему анализа неполадки и инструкции по устранению неполадок DNS с помощью стратегий отладки.

**Протокол передачи файлов (FTP)**
Этот раздел содержит информацию по устранению неполадок FTP, в том числе с помощью протокола задания сервера.

**Двухточечный протокол (PPP)**
Раздел содержит сведения об устранении наиболее распространенных неполадок PPP.

**Сервер почтового протокола (POP)**
Раздел содержит информацию по устранению неполадок сервера POP и других приложений, работающих с электронной почтой.

**Rexec**
Раздел содержит схему для локализации и устранения неполадок Rexec.

**Простой протокол передачи почты (SMTP)**
В разделе рассмотрены несколько способов устранения неполадок Простого протокола передачи почты (SMTP) и других приложений электронной почты.

**Telnet**
Раздел содержит информацию по устранению как общих неполадок Telnet, так и неполадок, связанных с типом эмуляции и сервером SSL. Кроме того, раздел содержит информацию о создании отчета о неполадках.

**Виртуальная частная сеть (VPN)**
В разделе приведены несколько стратегий устранения неполадок VPN, связанных с соединением, ошибками настройки, правилами фильтрации и др.

# Глава 4. Трассировка линии связи

Трассировка линии связи предназначена для устранения неполадок TCP/IP. Трассировка линии связи - это служебная функция, позволяющая отследить данные в линии связи, например в локальной сети (LAN) или глобальной сети (WAN). По окончании трассировки необработанные данные могут быть сохранены в потоковом файле, либо отформатированы и помещены в буферный файл для просмотра или вывода на принтер.

Трассировка линии связи может применяться для устранения неполадок как IPv4, так и IPv6.

Трассировку линии связи следует применять в следующих ситуациях:

- С помощью процедур анализа неполадки не удается получить достаточно информации о неполадке.
- Вы считаете, что причина неполадки - нарушение правил протокола.
- Вы считаете, что причина неполадки - помехи на линии.
- Необходимо проверить правильность передачи данных в сети приложением.
- Необходимо выяснить, не вызвана ли низкая производительность сети ее перегруженностью или низкой пропускной способностью.

Для запуска трассировки линии связи с помощью команд CL необходимы специальные права доступа *SERVICE, либо права доступа к функции Служебная трассировка OS/400 в Навигаторе iSeries. Дополнительная информация об этом типе прав доступа приведена в главе, посвященной пользовательским профайлам, руководства iSeries Security Reference  .

Вместо функции трассировки линии связи можно запустить во многом аналогичную команду Трассировка соединения (TRCCNN). Если приложения TCP применяют SSL или в системе применяется Защита IP, то данные, передаваемые линии связи, шифруются; функция трассировки линии связи не позволяет просмотреть такие данные. Напротив, команда TRCCNN выполняет трассировку данных до и после шифрования и, таким образом, может применяться в таких ситуациях. Вывод этой команды аналогичен выводу функции трассировки линии связи. Описание параметров и примеры приведены в Описании команды TRCCNN (Трассировка соединения) в разделе Интерфейсы прикладных программ (API).

Для применения функции трассировки линии связи необходимо выполнить следующие задачи:

**Планирование трассировки линии связи**
Предварительные операции, которые требуется выполнить до начала трассировки линии связи.

**Выполнение трассировки линии связи**
Операция трассировки линии связи.

**Дополнительные функции трассировки линии связи**
Дополнительные функции, связанные с трассировкой линии связи.

## Планирование трассировки линии связи

Прежде чем вы начнете работу с процедурой трассировки линии связи, выполните следующие действия:

1. Если библиотека IBMLIB или очередь вывода IBMOUTQ еще не были созданы, введите следующие команды:

```
CRTLIB LIB(IBMLIB)
CRTOUTQ OUTQ(IBMLIB/IBMOUTQ)
```

2. Для добавления библиотеки IBMLIB в список библиотек и выбора очереди IBMOUTQ в качестве очереди вывода задания введите следующие команды:

```
ADDLIBLE IBMLIB
CHGJOB * OUTQ(IBMLIB/IBMOUTQ)
```

3. Если файл принтера QTCPPRT отсутствует в системе, создайте его с помощью следующих команд:

```
CRTPRTF FILE(QTCP/QTCPPRT)  DEV(*JOB)
        RPLUNPRT(*YES) SCHEDULE(*FILEEND)
        FILESEP(0) LVLCHK(*NO)
        TEXT('Файл принтера TCP/IP')
CHGOBJOWN OBJ(QTCP/QTCPPRT) OBJTYPE(*FILE)
        NEWOWN(QSYS)
```

4. Для отправки буферного файла QTCPPRT, содержащего данные трассировки, в очередь вывода IBMOUTQ в библиотеке IBMLIB введите следующие команды:

```
OVRPRTF FILE(QTCPPRT) OUTQ(IBMLIB/IBMOUTQ)
OVRPRTF FILE(QPCSMPRT) TOFILE(QTCP/QTCPPRT)
```

   Переопределение параметров файла принтера не действует после завершения работы задания.

5. Выясните имя описания линии связи, сопоставленной с интерфейсом TCP/IP, вызывающим сбой или применяемым приложением или сетью, в работе которых возникает сбой. Для определения имени описания линии связи, сопоставленной с интерфейсом, введите команду NETSTAT *IFC.
6. Убедитесь, что линия связи подключена, и что интерфейс TCP/IP, применяющий эту линию связи, запущен. В этом случае система сможет передавать и принимать данные TCP/IP с использованием этих интерфейса и линии. Для проверки состояния интерфейса введите команду NETSTAT *IFC.

**Дальнейшие действия:**
Выполнение трассировки линии связи

## Выполнение трассировки линии связи

Трассировка линии связи выполняется с помощью команд CL. Трассировка линии связи подразделяется на следующие этапы:

1. Запуск трассировки линии связи
2. Завершение трассировки линии связи
3. Создание дампа трассировки линии связи
4. Печать результатов трассировки линии связи
5. Просмотр результатов трассировки линии связи
6. Чтение информации трассировки линии связи

## Запуск трассировки линии связи

Эта операция позволяет запустить трассировку для указанного описания линии или сетевого интерфейса.

**Примечание:** Функция трассировки линии связи больше не позволяет выполнять трассировку для описания сетевого сервера (*NWS). Трассировка может быть выполнена для описания линии (*LIN) или сетевого интерфейса (*NWI).

Для запуска трассировки линии связи выполните следующие действия:

1. В командной строке введите `STRCMNTRC`.
2. В параметре **Объект конфигурации** укажите имя линии, например `TRNLINE`.
3. В параметре **Тип** укажите тип ресурса: `*LIN` или `*NWI`.

4. В параметре **Размер буфера** укажите достаточный объем памяти для предполагаемого объема данных. Для большинства протоколов достаточно 8 Мб. Для протокола 10/100 Ethernet необходимо от 16 Мб до 1 Гб. Если вы точно не знаете необходимый объем памяти, укажите значение `16 Мб`.
5. Если при сборе данных необходимо ограничиться одним удаленным интерфейсом, укажите в параметре **Опции трассировки линии связи** значение `*RMTIPADR`. В противном случае, оставьте значение по умолчанию.
6. В параметре **Удаленный IP-адрес** укажите IP-адрес удаленного интерфейса, для которого будут собраны данные трассировки.

Трассировка линии связи продолжается, пока не будет выполнено одно из следующих условий:

- Будет запущена команда ENDCMNTRC.
- Выполнение трассировки будет прекращено из-за неполадки физической линии.
- Произойдет переполнение буфера - при условии, что в параметре **Переполнение трассировки** указано `*STOPTRC`.

**Дальнейшие действия:**
Завершение трассировки линии связи

## Завершение трассировки линии связи

Для форматирования и просмотра данных трассировки необходимо сначала завершить трассировку. Эта операция позволяет завершить процесс трассировки и сохранить данные буфера трассировки.

Для завершения трассировки линии связи выполните следующие действия:

1. В командной строке введите `ENDCMNTRC`.
2. В параметре **Объект конфигурации** укажите линию, для которой была запущена трассировка, например `TRNLINE`.
3. В параметре **Тип** укажите тип ресурса: `*LIN` или `*NWI`.

**Дальнейшие действия:**
Создание дампа трассировки линии связи в потоковом файле. Это необязательный этап, который, тем не менее, может оказаться полезным. Для того чтобы напечатать данные, не создавая дамп, перейдите к разделу Печать результатов трассировки линии связи

## Создание дампа трассировки линии связи

Если применяется IPv6, то следует создать дамп данных трассировки в потоковом файле согласно приведенным ниже инструкциям; если применяется IPv4, то эта операция является необязательной.

Создание дампа в потоковом файле дает некоторые преимущества. Эти преимущества рассмотрены ниже:

- Можно запускать новые трассировки, не теряя данных текущей трассировки.
- Данные трассировки можно форматировать несколько раз. Например, если одно из приложений применяет формат ASCII, а другое - EBCDIC, то вам потребуется отформатировать данные трассировки линии сначала в кодовой странице ASCII, а затем - в EBCDIC. Если данные трассировки хранятся в потоковом файле, то их многократное форматирование не представляет проблем.
- Данные трассировки сохраняются в случае IPL.
- Можно создавать вывод с помощью пользовательской программы форматирования.

Для создания дампа данных трассировки линии связи выполните следующие действия:

1. Создайте каталог, например `mydir`. Инструкции по созданию каталога приведены в Описании команды CRTDIR (Создать каталог) в разделе Управляющий язык (CL).

2. В командной строке введите DMPCMNTRC.
3. В параметре **Объект конфигурации** укажите линию, для которой была запущена трассировка, например TRNLINE.
4. В параметре **Тип** укажите тип ресурса: *LIN или *NWI.
5. В параметре **В потоковый файл** укажите полное имя файла, например /mydir/mytraces/trace1.

**Дальнейшие действия:**
Печать результатов трассировки линии связи

## Печать результатов трассировки линии связи

Результаты трассировки линии связи можно напечатать из двух различных источников, в зависимости от способа сбора данных. Вы можете напечатать либо собранные необработанные данные, либо содержимое потокового файла, в котором был создан дамп необработанных данных.

**Примечание:** Для того чтобы данные трассировки линии связи можно было напечатать из потокового файла, в системе должен быть установлен продукт Java (5722JV1).

Следующая операция записывает данные трассировки линии связи для указанной линии или описания сетевого интерфейса в буферный файл или файл вывода.

**Печать собранных необработанных данных:**

В случае, если необработанные данные были собраны без создания дампа, выполните следующие действия для их печати:

1. В командной строке введите PRTCMNTRC.
2. В параметре **Объект конфигурации** укажите линию, для которой была запущена трассировка, например TRNLINE, и нажмите Enter.
3. В параметре **Тип** укажите тип ресурса: *LIN или *NWI.
4. В параметре **Кодировка** укажите *EBCDIC или *ASCII. Данные следует напечатать дважды: один раз с опцией *EBCDIC, а другой - с опцией *ASCII.
5. В параметре **Отформатировать данные TCP/IP** укажите *YES и дважды нажмите Enter.
6. Повторите шаги с 1 по 5, указав другую кодировку.

**Печать содержимого потокового файла:**

В случае, если данные были сохранены в потоковом файле, выполните следующие действия для их печати:

1. В командной строке введите PRTCMNTRC.
2. В параметре **Из потокового файла** укажите полное имя файла, например /mydir/mytraces/trace1, и нажмите Enter.
3. В параметре **Кодировка** укажите *EBCDIC или *ASCII. Данные следует напечатать дважды: один раз с опцией *EBCDIC, а другой - с опцией *ASCII.
4. В параметре **Отформатировать данные TCP/IP** укажите *YES и дважды нажмите Enter.
5. Повторите шаги с 1 по 4, указав другую кодировку.

**Дальнейшие действия:**
Просмотр результатов трассировки линии связи

## Просмотр результатов трассировки линии связи

Для просмотра данных трассировки линии связи выполните следующие действия:

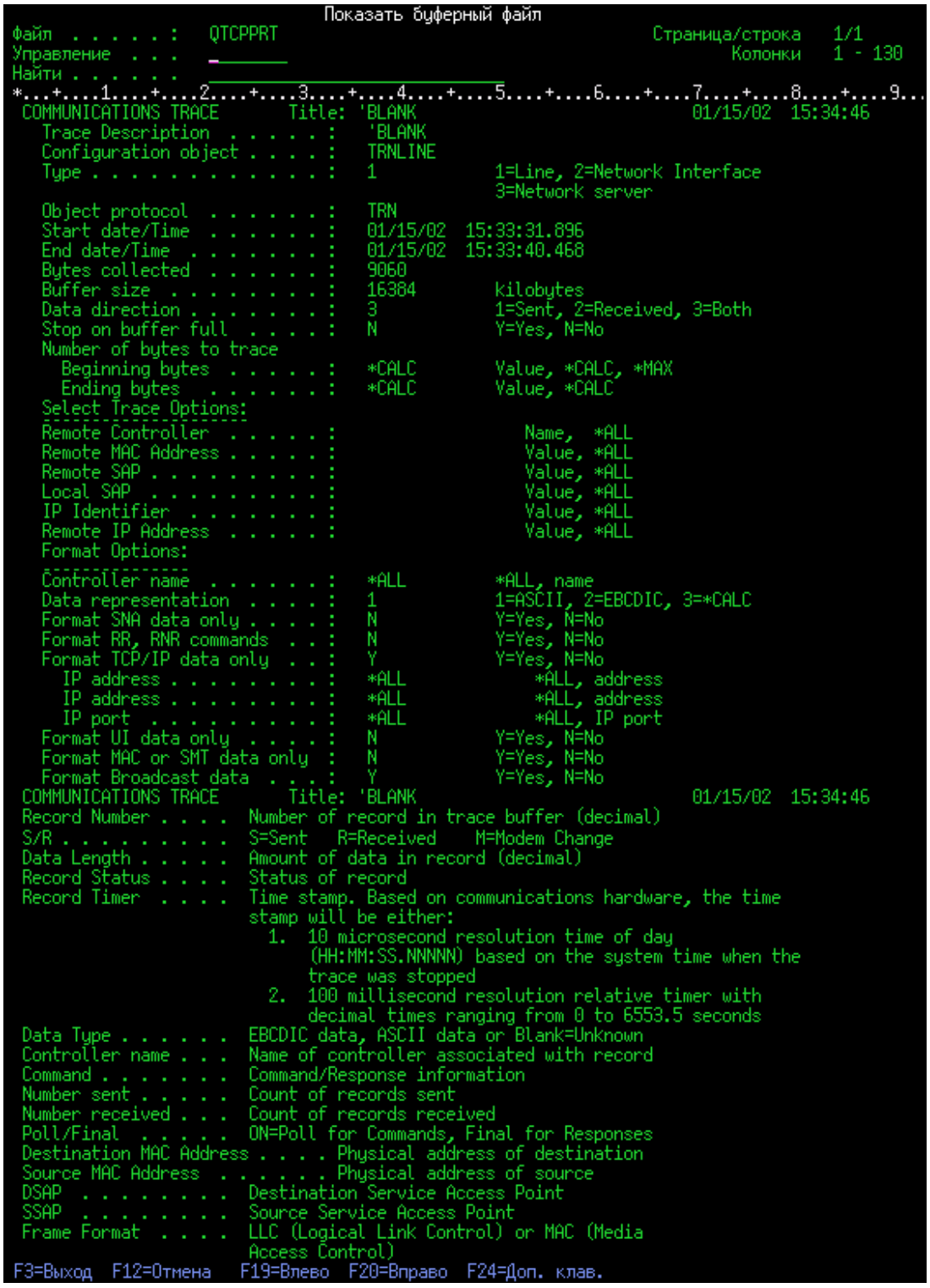
1. В командной строке введите WRKOUTQ OUTQ(IBMLIB/IBMOUTQ).

2. В окне **Работа с очередью вывода** нажмите клавишу F11 (Просмотр 2) для определения даты и времени создания необходимого буферного файла. Если нужного файла нет на экране и в нижней части меню показано слово Еще..., просмотрите остальные страницы меню; в противном случае перейдите к следующему шагу.
3. В столбце **Опц** введите 5 напротив буферного файла, который необходимо просмотреть. Чем ниже в списке находится файл, тем более свежие данные трассировки линии связи он содержит.
4. Убедитесь, что вы выбрали нужную информацию трассировки линии связи; проверьте также правильность времени запуска и завершения трассировки.

**Дальнейшие действия:**
Чтение информации трассировки линии связи

## Чтение информации трассировки линии связи

Информация трассировки линии связи подразделяется на несколько типов. В первой части этой информации выдаются параметры, указанные при запуске трассировки, например имя **Объекта конфигурации**. Далее приведен список элементов, таких как **Номер записи** и **S**/**R**, со связанными определениями; эти элементы являются заголовками последующих разделов данных трассировки линии связи. Этим списком удобно пользоваться при чтении данных трассировки. На следующем рисунке показана предварительная информация трассировки линии связи.



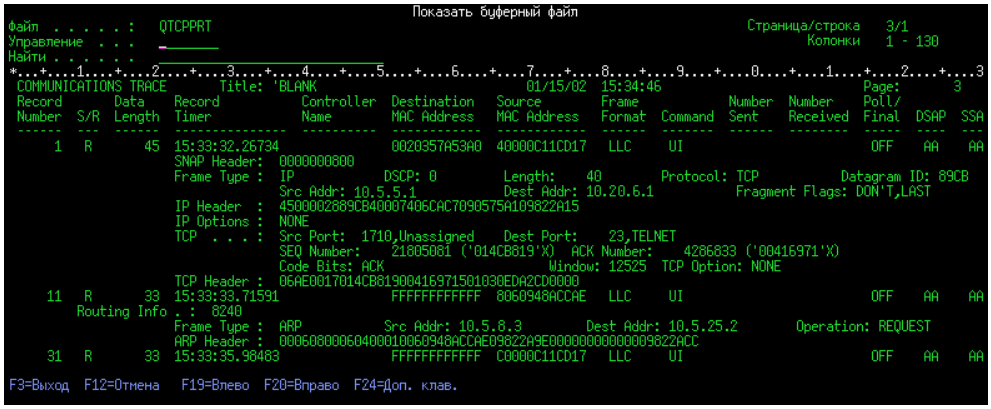

Ознакомившись с предварительной информацией, перейдите к собственно данным TCP/IP, полученным в результате трассировки линии связи. Заголовки, начинающиеся с **Номера записи**, обозначают разделы записей данных. Каждая пронумерованная запись соответствует кадру и содержит информацию об исходном и целевом IP-адресах, длине всей IP-дейтаграммы, типе обслуживания (TOS), исходном и целевом портах, а также номерах подтверждения (ACK). Эта информация поможет вам устранить ошибку TCP/IP в самой системе iSeries или в сети, к которой она подключена.

Символ звездочка (*), указанный после номера записи, например 31*, обозначает отсутствующие данные трассировки; это возможно в случае удаления записей трассировки. Сбор данных трассировки выполняется процессором ввода-вывода (IOP). Если линия связи сильно загружена, то IOP обрабатывает данные ввода-вывода в приоритетном порядке по сравнению с информацией трассировки линии связи. В этом случае, IOP может удалить некоторые записи трассировки линии связи. Это означает, что IOP не справляется с высокой скоростью или большим объемом данных, передаваемых по сети.

В случае отсутствия данных трассировки линии связи вы можете:

- Смириться с отсутствием некоторых кадров из-за того, что линия связи загружена.
- Выяснить, существует ли возможность переключить часть потока данных на другую линию или интерфейс TCP/IP.

На этом рисунке показана часть результатов трассировки линии связи, содержащая информацию о TCP/IP.




Процедура трассировки линии связи завершена.

Информация об удалении результатов трассировки, проверке состояния трассировки и определении объема памяти приведена в разделе Дополнительные функции трассировки линии связи.

## Дополнительные функции трассировки линии связи

Следующие команды и API обеспечивают дополнительные функции трассировки линии связи.

### Удаление результатов трассировки линии связи

Перед запуском новой трассировки линии связи вы должны удалить результаты предыдущей трассировки для этой линии. Удалить результаты трассировки можно в любой момент после ее завершения. Эта операция означает удаление буфера трассировки линии связи для указанной линии или описания сетевого интерфейса.

Для удаления результатов трассировки линии связи выполните следующие действия:

1. В командной строке введите DLTCMNTRC.
2. В параметре **Объект конфигурации** укажите имя линии, например TRNLINE.
3. В параметре **Тип** укажите тип ресурса: *LIN или *NWI.

### Проверка состояния трассировки линии связи

Вам может понадобиться информация о том, выполняются ли в данный момент какие-либо трассировки на сервере. Команда Проверить трассировку линии связи (CHKCMNTRC) возвращает

информацию о состоянии трассировки для указанной линии связи или описания сетевого интерфейса, либо о состоянии всех трассировок указанного типа, существующих на сервере. Информация о состоянии выдается в виде сообщения.

Для проверки состояния трассировки линии связи выполните следующие действия:

1. В командной строке введите CHKCMNTRC.
2. В параметре **Объект конфигурации** укажите имя линии, например TRNLINE, либо значение *ALL, чтобы проверить состояние всех трассировок определенного типа.
3. В параметре **Тип** укажите тип ресурса: *LIN или *NWI.

**Программная проверка объема памяти**

API Проверить трассировку линии связи (QSCCHKCT) позволяет выяснить максимальный объем памяти, выделенный для трассировок, а также размер в байтах объектов всех выполняющихся и остановленных трассировок на сервере. Дополнительная информация об API Проверить трассировку линии связи (QSCCHKCT) приведена в разделе Интерфейсы прикладных программ (API).

# Глава 5. Файлы конфигурации TCP/IP

При составлении отчета о неполадках TCP/IP необходимо включить в него копии файлов конфигурации, применяемых протоколом TCP/IP.Для создания копии файлов конфигурации TCP/IP выполните следующие действия:

1. Если библиотека IBMLIB или очередь вывода IBMOUTQ еще не были созданы, введите следующие команды:

   ```
   CRTLIB LIB(IBMLIB)
   CRTOUTQ OUTQ(IBMLIB/IBMOUTQ)
   ```

2. Для добавления библиотеки IBMLIB в список библиотек и выбора очереди IBMOUTQ в качестве очереди вывода задания введите следующие команды:

   ```
   ADDLIBLE IBMLIB
   CHGJOB * OUTQ(IBMLIB/IBMOUTQ)
   ```

   Для просмотра списка всех физических файлов, содержащих параметры конфигурации TCP/IP, введите следующие команды:

   ```
   WRKF FILE(QUSRSYS/QATOC*) FILEATR(PF)
   WRKF FILE(QUSRSYS/QATM*) FILEATR(PF)
   ```

   Для копирования содержимого файлов конфигурации вы можете выбрать опцию 3 (Скопировать) в меню Работа с файлами или вызвать для каждого такого файла указанную ниже команду, которая сохраняет копии файлов в отдельных буферных файлах в очереди вывода IBMOUTQ.

   ```
   CPYF FROMFILE(QUSRSYS/QATOCHOST) TOFILE(*PRINT)
        FROMMBR(*ALL)  TOMBR(*FROMMBR)
        MBROPT(*ADD) CRTFILE(*NO) OUTFMT(*HEX)
   ```

# Глава 6. Протокол работы продукта

Каждый раз, когда дейтаграмма TCP/IP отклоняется из-за ошибки протокола, код LIC TCP/IP создает запись об этом в протоколе работы продукта.

Для внешних дейтаграмм TCP/IP примером такой ошибки протокола может быть сбой при попытке установить соединение X.25, по которому должны передаваться эти дейтаграммы. В этом случае, пользователь получит сообщение об ошибке, и дейтаграмма будет отклонена.

При работе с внутренними дейтаграммами запись будет создаваться в Протоколе работы продукта только при выполнении обоих следующих условий:

- Атрибут Заносить в протокол ошибки TCP/IP установлен в *YES.
- Дейтаграмма не прошла один из тестов допустимости протокола TCP/IP, определенных в RFC 1122, и в результате была отклонена системой. (**Отклонение дейтаграммы без уведомления** означает, что принятая дейтаграмма будет отклонена, и отправившему ее удаленному хосту не будет возвращено сообщение об этом.) Например, дейтаграмма может быть отклонена, если ее контрольная сумма или целевой адрес окажутся недопустимыми.

При отклонении дейтаграммы описанным выше образом заголовки дейтаграмм IP и TCP/UDP добавляются в запись Протокола работы продукта. Справочный код для записей Протокола работы продукта - 7004.

Напечатано в Дании